Aalto University School of Electrical Engineering
Department of Communications and Networking

Wireless Localization in Narrowband-IoT Networks

Mcha Khamis

Master's Thesis submitted in partial fulfilment of the requirements for the Degree of Master of Science in Technology

Espoo July

Supervisor: Professor Olav Tirkkonen

Advisor: Nicolas Malm.

Aalto University **Abstract of the Master's Thesis**

Author: Mcha Khamis

Title: Wireless Localization in Narrowband-IoT Networks

Date: July 2020 **Number of pages:** 44

School: Electrical Engineering
Professorship: S-72 Communications Engineering

Supervisor: Professor Olav Tirkkonen

Instructor: M.Sc Nicolas Malm

Abstract

Internet of things (IoT) is an emerging technology which connects devices to the internet and with the upcoming of 5G, even more devices will be connected. Narrowband-IoT (NB-IoT) is a promising cellular technology that supports the connection of IoT devices and their integration with the existing long-term evolution (LTE) networks. The Increase of location-based services that requires localization for IoT devices is growing with the increase in IoT devices and applications. This thesis considers the localization of IoT devices in the NB-IoT wireless network. Localization emulation is produced in which Software Defined Radio (SDR) used to implement Base stations (BS) and user equipment (UE). Channel emulator was used to emulate wireless channel conditions, and a personal computer (PC) to calculate the UE location. The distance from each BS to the UE is calculated using Time of arrival (TOA). Triangulation method used to estimate the UE's position from the different BSs distances to the UE. The accuracy of positioning is analysed with various simulation scenarios and the results compared with third generation partnership project (3GPP) Release 14 standards for NB-IoT. The positioning accuracy requirement of 50 m horizontal accuracy for localization in NB-IoT 3GPP standardized have been achieved, under Line of Sight (LOS) full triangulation scenarios 1 and 2.

Keywords: IOT, 5G, NB-IOT, SDR, UE, TOA, localization,3GPP

Acknowledgment

I would like to express my gratitude to Prof. Olav Tirkkonen for granting me the opportunity to work on this project and his guidance throughout the thesis. My grateful thanks also extend to M.Sc. Nicolas Malm for providing me lots of valuable advice and comments in the thesis. Also, I would like to thank Viktor for allowing my longer stays at the lab. I would also like to thank Postdoc Hanan Al-Tous for her valuable remarks and feedback on my thesis writing. Thanks to my fiancé for providing me with her emotional support and devotion, and to my dad for his continuous encouragement in my entire academic life.

Finally, I want to thank God for granting me the opportunity to be here in such a great place.

Espoo, 31 July 2020

Mcha Khamis

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
AOA	Angle of Arrival
API	Application Programming Interface
BS	Base Station
CAT-M1	User equipment Category M1
CP	Cyclic Prefix
eDRX	Extended Discontinuous Reception Transmission
FDD	Frequency Division Duplex
GDOP	Geometrical Dilution of precision
GPS	Global Positioning Systems
GPSDO	GPS-disciplined oscillator
IFFT	Inverse Fast Fourier Transform
IoT	Internet of Things
ISM	Industrial Scientific and Medical
LoRaWAN	Low Range Wide Area Networks
LOS	Line of Sight
LWPAN	Low Power Wide Area Networks
LTE	Long-Term Evolution
LTE-M	Long-Term Evolution Machine Type Communication
M2M	Machine-to-Machine Communication
MTC	Machine-type Communication
NB-IoT	Narrow Band Internet of Things
NLOS	Non-Line-of-Sight
NPRS	Narrowband Positioning Reference Signal
OFDMA	Orthogonal Frequency division multiple access
PC	Personal Computer
PPS	Pulse per Second

PRB	Physical Resource Blocks
RSS	Received Signal Strength
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDR	Software-Defined Radio
SNR	Signal to Noise Ratio
TDOA	Time Difference of Arrival
TOA	Time of Arrival
TOF	Time of Flight
UE	User Equipment
UHD	USRP Hardware Driver
USRP	Universal Software Radio Peripheral
VoLTE	Voice over LTE
3GPP	Third Generation Partnership Project

LIST OF NOTATIONS

N_{ID}^{NPRS}	NPRS identification number
N_{ID}^{cell}	Physical layer cell identity
N_{RB}^{DL}	Downlink bandwidth configuration, expressed in multiples of N_{SC}^{RB}
N_{RB}^{UL}	Uplink bandwidth configuration, expressed in multiples of N_{SC}^{RB}
$N_{RB}^{max,DL}$	Maximum downlink of resource block
N_{SC}^{RB}	Resource block size subcarriers
N_{symb}^{DL}	Number of OFDM symbols in a Downlink slot
v_{shift}	Variable frequency shift

1 Introduction

In recent years, the Internet of Things (IoT) has become one of the significant trends in technology, and the number of IoT devices is expected to reach 150 billion by 2025 [1]. The goal of IoT is to connect every device that can benefit from an internet connection, ranging from low complexity sensors to complex self-driving cars.

Therefore, the IoT network environment usually has a standard set of characteristics which vary according to their application; however, large number of devices are connected which exhibit the characteristics of low power and low complexity. One category of IoT focuses on such devices which are connected in large numbers in a network; this is known as massive IoT. Large numbers of devices are connected in a network in which they have a low transmission rate and long battery life.

The current expansion of massive IoT has accelerated the emergence and standardization of communication protocols which might better suit these network characteristics. These massive devices need a communication protocol, one of the emerging protocols is Narrowband-IoT.

Narrowband-IoT is a radio technology that facilitates the communication of IoT devices in low power wide area networks (LPWAN). These massive IoT devices typically use sensors in a node network. These IoT devices rely heavily on localization, which means identifying the current position of the device itself. However, the enormous number of these devices in a network (dense networks) impedes the practicality and increases the cost of installing global Positioning systems (GPS) on each device [2]. Moreover, the nature of the environment decreases the efficiency of GPS finding the exact location of the device as it may be inside a factory or behind concrete walls. As manual localization of the devices is an absolute impossibility, it heightens the need for localization technology that can work with this type of network's requirements

This Thesis aims to test and evaluate the performance of NB-IoT in the localization of IoT devices. The scope of the thesis is limited to NB-IoT localization in Release 14 of 3GPP [3] and the introduction of Narrowband positioning reference signal (NPRS) in positioning. Implementation of NPRS is made using MATLAB, a small NB-IoT network is done using software-defined radio (SDR) and wireless channel emulator, where the user equipment (UE) is localized in different scenarios.

1.1 Thesis organization

The thesis is organized as follows: Chapter 2 introduces IoT and provides an overview of NB-IoT and compares it with Long Term Evolution-Machine Type Communication (LTE-M). The concepts and the algorithms for localization are investigated in Chapter 3. Chapter 4 discloses the NB-IoT positioning and general architecture, whereas Chapter 5 provides the design and setup of the localization environment. The emulation and its results are shared in Chapter 6. Finally, Chapter 7 concludes and summarises the thesis.

2 Background

2.1 Internet of things

Started as sensors sending data and simple machine to machine communication, IoT has progressed far in the last decade. IoT devices are getting more complex beyond sensors to smart devices. Managing the communication and the connection of such devices is adding higher value to the devices and more features to its users. IoT expanded the domain of embedded devices; embedded devices are devices with a specific purpose that we usually integrate with a bigger system, such as, motion detector sensor in automatic gates. By connecting them to the internet, we get more remote control of the device and have a way of analysing more of the device data and learning more about its behaviour.

IoT in healthcare is transforming the healthcare industry as it is enhancing the effectiveness of medical equipment. Constant monitoring, tracking, and connecting patient with the healthcare system are saving time and lives. All patients' vitals can be collected by sensors regularly and sent to the doctor, cutting down chains of intermediate people slowing information reach. Such as, an abnormal increase in a patient glucose level or heartrate can instantly trigger an alarm even if the patient is not physically in the hospital. IoT provides a more defined and detailed digital history of patient records, diagnosis, therapy, medications, and recovery [4]. This history is now being used by Artificial Intelligence (AI) to predict the likelihood of occurrence of certain diseases or the recovery from them.

IoT in smart wearables, nowadays, more and more people are using intelligent wearables into their everyday lives [2]. Rings that can monitor sleep cycles and trace sleep patterns, watches that can track personal training and overall activity while also pay for the food at the grocery.

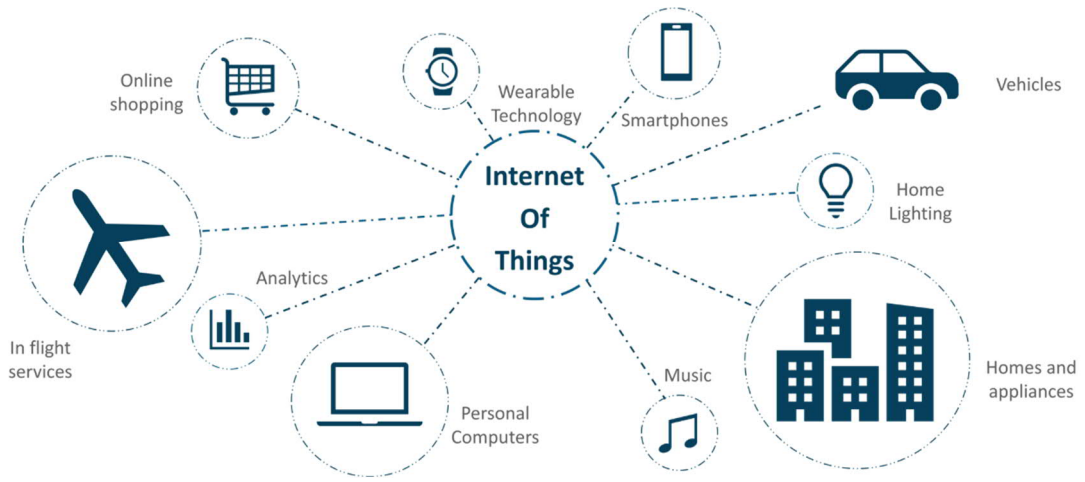


Figure 2.1 IoT use cases [5]

IoT in industry, IoT has numerous use cases in various aspects of the industry. Although industry use cases differ from personal or urban uses cases of IoT as it uses mainly.

IoT in smart cities, many intelligent cities architecture envision IoT in its infrastructure. Bright lighting being the recent trend where many lighting systems evolved to make smart lighting decisions by use of IoT [6]. Light sensors and controllers automatically adjust light intensity by the time of the day. The lighting user habits and preferences that we saved as patterns and extracted it from user data for later saving and automatic adjustments are to improve the quality of the user experience. Air quality, IoT is used to improve air quality, temperature, carbon dioxide, humidity, etc., are detected by sensors that we connected to the internet. These sensors detect and adjust air quality, accordingly, warns against certain threshold levels and collect data [7].

2.2 Narrowband IoT

Third generation partnership project (3GPP) standardized Narrow band – IoT (NB-IoT) and Long-Term Evolution Machine Type Communication (LTE-M) as cellular Low Power Wide Area Networks (LPWAN) used to address the communication and services of IoT devices. On the other hand, proprietary LPWAN standards were made by private companies in an unlicensed Industrial Scientific and Medical (ISM) band for IoT communication, such as, SigFox and Low Power Wide Area (LoRaWAN) [8].

NB-IoT focuses on connecting a massive number of low complexity devices that transmit a small quantity of data overstretched periods. It allows the devices to benefit from the full availability of cellular communication, not limiting the devices to a particular place or area as with short-range communication protocols, such as Bluetooth and eliminating the need of cable connection.

NB-IoT has 180 kHz channel band width hence the name “narrowband”, which makes it efficient in reducing the consumption of the radio spectrum while deploying a mass number of devices. NB-IoT provides the benefit of smoothly integrating with existing LTE as its architecture utilise most of the LTE core specifications. It uses the same LTE channel modulation orthogonal frequency division multiple access (OFDMA) for downlink (DL) and single carrier- frequency division multiple access (SC-FDMA) for the uplink (UL). Also, the same coding schemes, rate matching and interleaving as LTE [9]. NB-IoT support frequency-division duplex (FDD) but only half-duplex (HD) systems.

NB-IoT has three modes of deployment which provide flexibility to various deployment needs. For in-band deployment, the NB-IoT carriers are inside LTE carriers, for Guard-band deployment the NB-IoT carriers are between guard bands of LTE carriers and for Standalone deployment the NB-IoT has its own assigned carrier. In-band and Guard-band deployments both utilise LTE hardware. This enables lower cost and fast implementations of NB-IoT infrastructure, also excel in the development of its products and software.

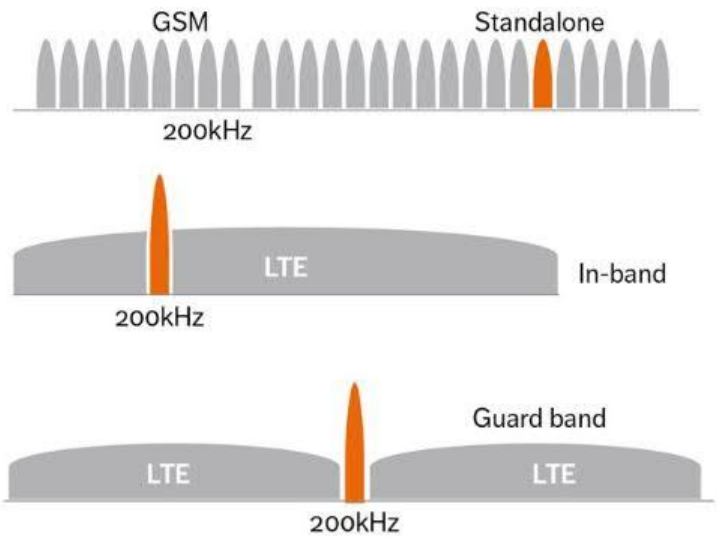


Figure 2.2 NB-IoT modes of operation [10]

2.3 LTE-M

The LTE-Machine Type communication (LTE-M) is introduced in LTE release 13 [11] by 3GPP alongside with NB-IoT as a cellular technology for IoT. LTE-M produced a new UE category called mobility category (Cat-M1). On contrast to NB-IoT, Cat M1 is made for high data applications. It supports up to 1 MB/s data rate and has 1.4 MHz bandwidth channel [12]. These characteristics made it more fit with smart devices applications rather than simple sensors. In the meanwhile, NB-IoT UE (NB1) only operates in 200 kHz channel bandwidth that is mostly used by low-complexity devices. These devices applications do not have a harsh low latency policy or a reliable data rate requirement. Cat-M1 also supported additional features that were not implemented by NB-IoT. Voice over LTE (VoLTE) was introduced by Cat-M1, allowing voice calls for IoT devices. This feature is nourishing the smart wearable industry as it will enable more devices to make calls besides the mobile phone. Handover feature permitting seamless movement of devices between cells without breaking the connection [12]. Last, cat-M1 introduced positioning, opening the door to more tracking IoT devices and location-based applications [13].

On the other hand, Cat-M1and NB-IoT shares some standard features that give them advantages in the IoT industry. First, they both support enhanced signal coverage per base station, and this feature is more critical in the industry as IoT devices may be in weak coverage areas, such as basement or under heavy machinery. Moreover, they both decrease power consumption by making power saving modes. Most IoT devices run on batteries, and battery life is a critical aspect in the design of IoT devices hardware as well as software. Lastly, they both supports extended discontinuous reception transmission (eDRX). In Which devices have extended sleeping modes so with an active window for transmission and reception while the rest of the time is sleeping to save battery and free bandwidth for other devices [13].

Figure 2.3 NB-IoT Vs LTE-M use cases [12]

The 3GPP standard introduced a new LTE-M category Cat-M2 in LTE release 14 [3]. Cat-M2 provides a higher data rate than Cat-M1, 7Mb/s for uplink and 4Mb/s downlink, and this enables Cat-M2 devices to run more applications that require higher throughput, such as video transmission. In conclusion, NB-IoT and LTE-M are both radio technologies for IoT communication and applications. They both serve massive number of connected devices (massive IoT) that are mostly running on batteries and

can be used in areas of weak coverage areas. LTE-M with both its UE categories M1 and M2 are more fit for high data rate applications as; video surveillance, smart wearables and connected vehicles. NB-IoT addresses more low-cost and low complexity devices like sensors, gadgets and meters that don't need to send high data rates but need to deploy in massive amount. The typical use case would be smart metering or smart parking where a small sensor is required to report data at regular intervals informing about the change in sensor state providing a new information or allowing the device to make the decision.

2.4 Localization and IoT

Finding the location of any device or asset and being able to track it is valuable treats in trading and industry. Logistics and supply chain management depends heavily on positioning, where there is a constant need to find the current location of cargo for shipping, retrieving, and storing. On the other hand, localization is finding opportunities for use outside the industry. Livestock tracing is using positioning, and animal research is finding localization beneficial in studying wild animals in its natural habitat [14]. Added to that, smart wearables are starting to develop location-based applications where the location is a critical value for such service [2].

IoT can greatly benefit localization and tracing are various industrious and for different use cases. The added value of internet connection provided by IoT is flourishing localization by giving it more up to date location and exact path of the route of the object we tracked while making this information widely available for infinite observers.

For the industrious benefits of localization discussed above, and its IoT use cases, it is the primary purpose of this thesis study. Specifically, in NB-IoT communication systems. As with the characteristics of the NB-IoT briefly discussed, we can have an idea about the nature of such localization. Unlike GPS, NB-IoT localization is not as precise. As the nature of NB-IoT system is not time-critical, and devices often sleep. Moreover, it is most probably two-dimension positioning, as most NB-IoT devices are on 2D planes and never fly. Last, it is not a continuous tracing as NB-IoT devices are mostly stationary and do not autonomously change position often unless moved by the owner.

3 Localization Algorithm & Range Measurement Techniques

3.1 Triangulation Algorithm

Multilateration is a process by which the position of an unknown object can be determined through its distance from known reference points positions. Triangulation is a special case of multilateration where the number of the reference points are three, and they form a triangular shape around the object [15]. In this thesis, these reference points are Base stations, and they send signals to the desired object UE. The distance between each reference point and the target object is calculated through range measurement techniques; Time of Arrival (TOA), Time Difference of Arrival (TDOA), Angle of Arrival (AOA), Received Signal Strength (RSS) [16]. Triangulation use triangle properties and trigonometric functions to calculate the target position. The geometric solution represents each reference point as a centre of a circle, the radius of the circle being the distance between the reference point and the target object. The three circles intersect at a point, and this point is the estimated position of the localized object.

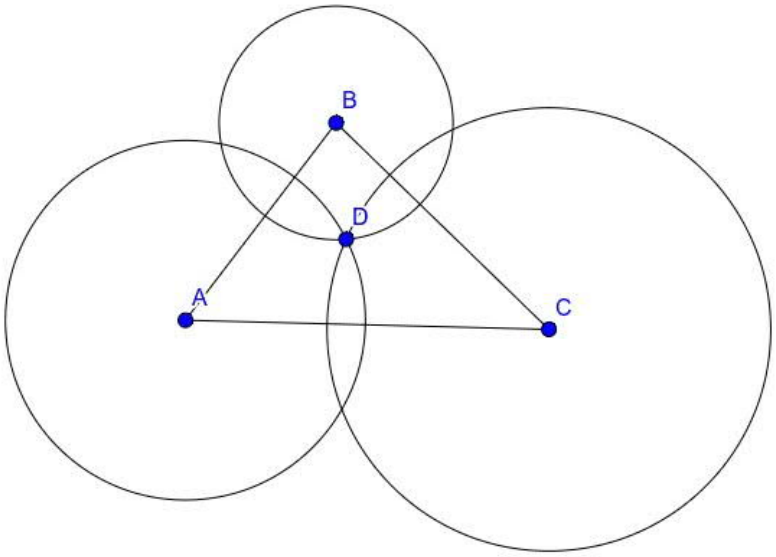


Figure 3.1 Triangulation [17]

Let the reference points be (A, B, C) at positions A(x_1 , y_1) , B(x_2 , y_2) ,C(x_3 , y_3) , the distance between each base station and the UE is d_i and the UE position coordinates (x, y). The distance d between the base station and the UE is calculated as follows:

$$d_1 = \sqrt{(x - x_1)^2 + (y - y_1)^2} \quad (1)$$

$$d_2 = \sqrt{(x - x_2)^2 + (y - y_2)^2} \quad (2)$$

$$d_3 = \sqrt{(x - x_3)^2 + (y - y_3)^2} \quad (3)$$

Solving those three equations for (x, y) leads to the estimated location of the device [18].

3.2 TOA

TOA measures the Time of Flight (TOF) t taken for the signal to travel from the Base station to the UE, which is directly proportional to the distance between them. The signal travels at a speed of light $c \sim 2.98 \times 10^8\, m/sec$ and the distance d can be measured as in equation.

$$d = c \times t \quad (4)$$

TOA measures the time of one-way propagation of the signal and not the round-trip time. This requires the synchronisation of all the clocks of Base stations and the UE. TOA corresponds to a circle where the Base station is at its centre and radius is d. The UE lies on the circle, but the exact location cannot be found with just one Base station. Even two Base stations could not locate the UE as two base station can intersect at two different places.

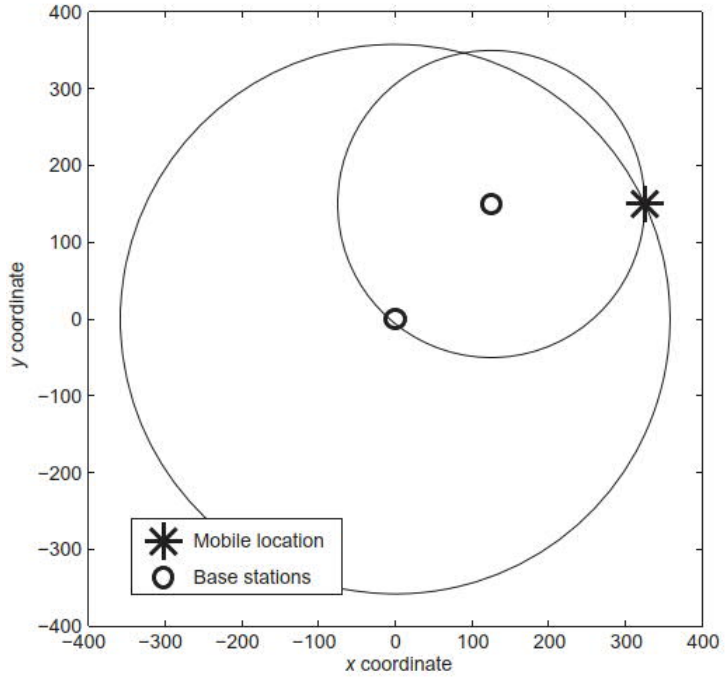


Figure 3.2 Two Base stations intersection

At least three Base stations are needed for the UE localization so three circles can intersect at one location as in Figure 3.1. However, in the presence of noise or low Signal to Noise (SNR) ratio circles may not intersect at a single point or may intersect at multiple points. Hence adding more Base stations to UE localization using TOA is beneficial in yielding more accurate results.

3.3 TDOA

TDOA is similar to TOA in which it uses the Base stations of known locations to send signals to the UE to estimate the distance. However, it does not directly use TOA but calculate the time difference of arrival of two Base stations to estimate the UE distance. TDOA advantage over TOA is that the Base stations do not need to synchronize clocks with the UE, so it is less complex.

TDOA uses hyperbolic mathematical principles to estimate the position of the UE [15]. The first Base station is considered a reference base station and the TOA is estimated normally. The second Base station will form a hyperbola using TDOA measurement with respect to the reference Base station.

Third Base station will form another hyperbola using TDOA measurement with respect to the reference signal. The intersection point of the two hyperbolas is the estimated UE location.

let the transmission of signal be at the time t_M and τ_i be the TOF of the i[th] Base station located at position (x_i , y_i). The TOA of the i[th] Base station t_i is given by

$$t_i = \tau_i + t_M \tag{5}$$

$$= \frac{d_i}{c} + t_M \tag{6}$$

$$= \frac{\sqrt{(x - x_i)^2 + (y - y_i)^2}}{c} + t_M \tag{7}$$

Applying TDOA and subtracting the reference signal TOA we eliminate start time t_M

$$t_i - t_j = \tau_i + t_M - (\tau_i - t_M) \tag{8}$$

$$= \tau_i - \tau_j \tag{9}$$

$$= \frac{d_i}{c} - \frac{d_j}{c} \tag{10}$$

$$= \frac{\sqrt{(x - x_i)^2 + (y - y_i)^2} - \sqrt{(x - x_j)^2 + (y - y_j)^2}}{c} \tag{11}$$

We still have one equation with two unknowns, and so we have an infinite number of solutions, so we take a third Base station and compute the TDOA with reference signal.

$$t_i - t_j = \frac{\sqrt{(x - x_i)^2 + (y - y_i)^2} - \sqrt{(x - x_j)^2 + (y - y_j)^2}}{c} \tag{12}$$

$$t_i - t_k = \frac{\sqrt{(x - x_i)^2 + (y - y_i)^2} - \sqrt{(x - x_k)^2 + (y - y_k)^2}}{c} \tag{13}$$

3.4 AOA

Angle of arrival measurement, also known as direction of arrival or bearing, is a technique that calculates signal angles for determining its distance from the Base station.

Two main measurement techniques are used for angle calculation, antenna phase response and antennas amplitude response [16]. AOA uses on multiple-element antenna array which measures the received signal amplitude, phase at each element to draw the LOS path of the transmitter. At least another antenna is needed to draw another LOS path, and the intersection of those two LOS paths is the estimated target location. AOA is less complex than TOA and TDOA and does not require base station synchronization. Moreover, an estimation of the target location can be done with only two Base stations. However, installation of antenna array at each Base station is required. Although there is an additional cost of directional, it eliminates interference coming from signals of unwanted directions. A significant drawback of AOA is the decrease of localization efficiency with distance. As with longer distances between the UE and Base station alter the propagation characteristics of the incoming signal [15].

3.5 RSS

Received signal strength measure the incoming signal strength in estimating the distance between the Base station and the UE. Signal strength indicates how far the signal travels in an inversely proportional relation between signal strength and distance. Signal strength is measured by the average signal power received in the receiving antenna with relation to the transmitted power at the transmitting one. Power of the transmitted signal decreases according to a decay model in which distance travelled by the signal, transmitted power and a path loss constant contributes to the final received signal power. After RSS measurement, the distance between the UE and Base station is estimated, and at least three Base stations are required to estimate the location of the UE similarly to TOA. RSS method does not require synchronization of Base station clocks which yields a less complex method for localization [16].

One major disadvantage for RSS measurement is the alteration of signal properties with environment or obstacles collision [19]. The transmitted signal may get reflected, deflected, or refracted affecting its power characteristics. Signal propagation issues significantly affect the signal strength received Signal Multipath in which different copies of the same signal take different paths and can defect the resultant received signal. Shadowing in which signal hits a huge obstacle preventing its path to a receiver behind it. Signal attenuation due to environmental channel conditions such as rain. Furthermore, power control mechanisms used by base stations may mislead distance estimation and target localization leading to inaccurate results. All previously mentioned factors decrease the efficiency of the RSS in distance estimation.

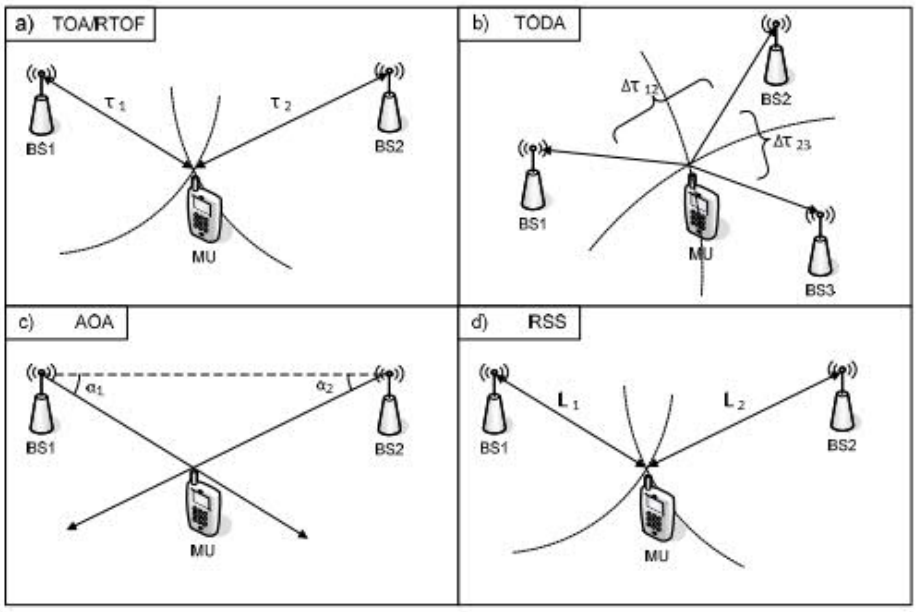


Figure 3.3 Triangulation range measurements [20]

4 Design and Implementation

4.1 Experiment design

The main purpose of this chapter is to describe the implementation of a real-time emulation of the localization system. The emulation comprises of main parts; the base stations are responsible for localization, the localized object (UE), the radio environment where the localization takes place, time delay calculation and position estimation.

The base stations are time-synchronized with each other and simultaneously send Narrowband positioning reference signals (NPRS) to the UE. The host computer at the UE calculates the time delay of different base stations from the received NPRS signal, then it uses the triangulation algorithm for position estimation of the UE.

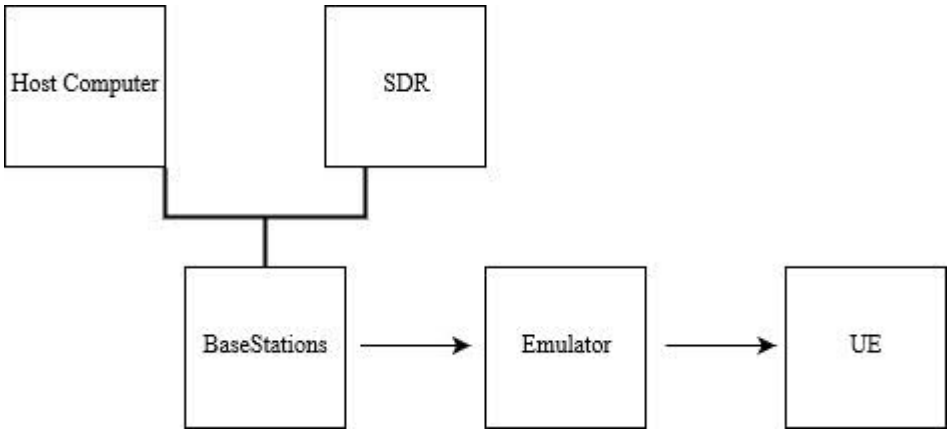


Figure 4.1 Experiment setup

4.1.1 Base-stations

Base-stations are responsible for generating and sending NPRS signals to the UE. In this implementation, a base-station consists of a computer acting as a processing unit connected to a software-defined radio (SDR), which acts as the transceiver sending and receiving NPRS signals between Base stations. The SDR device used is Universal Software Radio Peripheral (USRP) developed by Ettus Research [21].

USRP is a radio front-end device that transmits and receives radio signals generated by the host computer. The host is connected to the USRP through Gigabit Ethernet and communicates with the USRP through application programming interface (API) that accesses the USRP Hardware Driver (UHD) [22].

Figure 4.2 USRP Device [23]

UHD API allows the host to connect and control the SDR by developing UHD-based applications. These applications implement specific functionalities to configure the device's role. The UHD APIs use C++ programming language. In this setting, there are two main UHD applications running by the USRPs, the transmitter script, which is used primarily by the base station and the receiver script, which is used by the UE. Although the two programs perform different tasks, they share common basic settings such as, the device arguments, frequency, sampling rate, bandwidth, RF gain. The used frequency is set at 400 MHz, although signals were not wirelessly transmitted, but the generated signal is transmitted through a cable to an emulator is used to model the channel. The sampling rate $1.92\ {Megasamples}/{sec}$ chosen to fit with the NB-IoT frame structure mentioned in [3], the bandwidth is 1_{MHz} and the channel gain is set to 10_{db}

USRPs send and receive the desired signal as interleaved in-phase (I) and quadrature (Q) samples. The TX script reads IQ samples from a written file. Samples are stored in an array and then uploaded to a buffer where a transmitter stream is transmitted. The RX script receives the IQ samples where the samples are downloaded to a buffer and then written to a file.

All the USRPs acting as base stations are synchronized to a common timing source to estimate the time of arrival accurately. This synchronization is achieved by an OctoClock-G CDA-2990 [24] .It is a device which provides distribution system and timings reference. It distributes 10 MHz and 1 pulse per second (PPS) signals generated from an internal GPS-disciplined oscillator (GPSDO). GPSDO is synchronized to GPS timing standard and can align multiple systems with accuracy of approximately 50 ns.

4.2 NB-IoT Downlink Waveform and NPRS

The LTE MATLAB toolbox [25] is used to generate NB-IoT standard complex baseband waveform for test and measurement applications. NB-IoT downlink waveform [26] is standard compliant with LTE-Advanced Pro Release 13 [11]. The waveform is 180 kHz narrowband carrier, consists of physical layer channels, and signals with a full resource element grid. It supports three NB-IoT modes of operation: Standalone, Guard-band and In-band. The Standalone operation mode provides a separate carrier for NB-Iota to be deployed away from the LTE spectrum while the In-band mode deploys NB-Iota in the same LTE carriers where it shares LTE resource blocks. Guard-band operation mode deploy NB-Iota carrier in LTE guard-band between carriers.

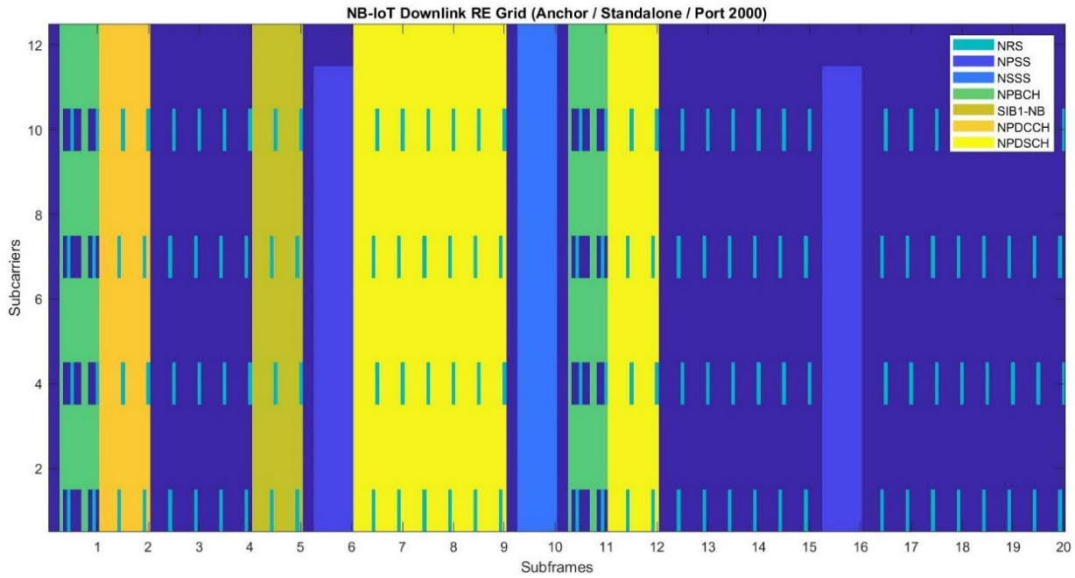


Figure 4.3 NB-IoT Downlink Waveform

In this emulation, MATLAB NB-IoT waveform is used as a carrier for the NPRS signals. Although the waveform is generated according to [11] before the emersion of NPRS, NPRS signals are generated separately and mapped onto empty sub-frames of the waveform. The standalone mode is selected because it provides the least Interference with existing LTE deployments.

NPRS generated according to LTE Release 14 [3]and mapped onto the downlink sub-frames of the waveform. Mapping is done according to [3] where NPRS is only transmitted in NB-IoT carrier resource blocks reserved for NPRS transmission. Two mapping sequences are defined, one for the In-band and another for standalone and guard-band modes of operation. The main difference is that In-band mode cannot allow all OFDM symbols to be used for NPRS transmission while standalone, Guard-band can allow for full NPRS symbols usage, especially when there is no data transmission.

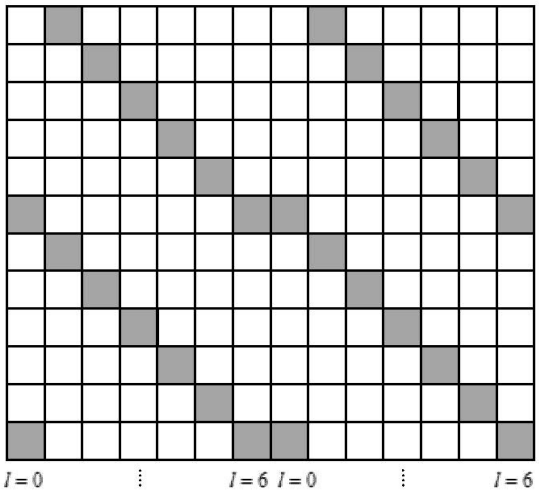


Figure 4.4 NPRS mapping in Standalone operation mode

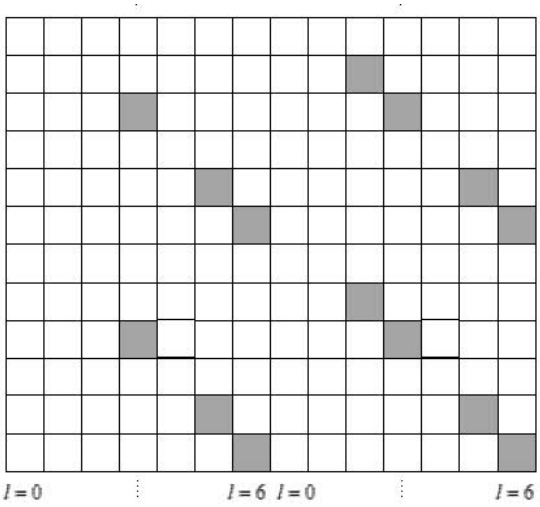


Figure 4.5 NPRS mapping in In-band operation mode

Figures 4.4 & 5.5 above show the resource grid of Standalone and In-band modes, respectively. The grey squares represent the NPRS position, each element in the resource grid is called resource element and identified by the index pair of (k, l) where k and l are indices in the frequency and time domain, respectively. Resource element used for NPRS transmission on any antenna port cannot be used for any transmission on any other antenna port in the same slot.

The NPRS sequence $r_{l,ns}$ (where is n_s slot number within the radio frame, l is the OFDM symbol number within the slot) is mapped to the complex-valued modulation symbol [3].

	$\alpha_{k,l}{}^{(p)} = r_{l,ns}(m')$	(14)

The resource element (k, l) on antenna port p corresponds to the complex value $\alpha_{k,l}{}^{(P)}$

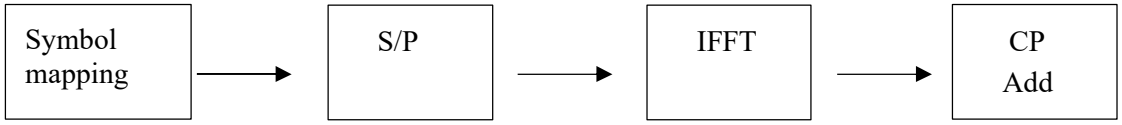
	$k = 6m + (6 - l + v_{shift}) mod\ 6$ $l = 1, 2, 3, 4, 5, 6$ $m = 0, 1$ $m' = m + N_{RB}^{max,DL} - 1$ $v_{shift} = N_{ID}^{NPRS}\ mod\ 6$ $N_{ID}^{NPRS} = N_{ID}^{Ncell}$	(15)

The variable v_{shift} define the position in the frequency domain for different reference signals. Frequency shift v_{shift} reduce interference between adjacent NPRS signals by allowing up to six different cells to transmit NPRS signals on different subcarriers so they do not overlap in the frequency domain.

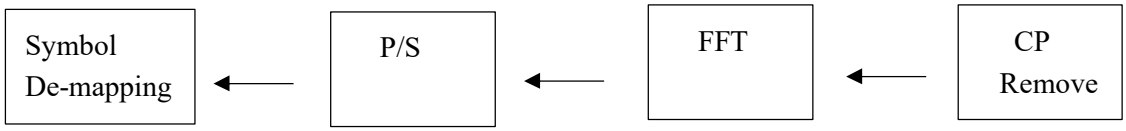
4.2.1 OFDM transmitter

After mapping of the NPRS signal on the NB-IoT downlink waveform, the produced grid is passed to an OFDM transmitter [27]. The OFDM transmitter's main purpose is to convert a serial stream of symbols into parallel sub streams. First data is packed into FFT buffers and reordered. An IFFT operation is performed on each symbol, and cyclic prefix is added at the end by coping the last samples of the IFFT output to the beginning of the buffer. The output IQ samples are normalized and interleaved I and Q before being written to a file and transmitted through the UHD.

OFDM Transmitter



OFDM Receiver



Symbol mapping performs mapping on binary data bits to be mapped to a complex-valued number on the resource grid. The second stage serial-to-parallel converter converts serial symbol sequence into parallel sequence and reorganizes the order of data symbols into smaller subset of data symbols. The third and main stage is the Inverse Fourier Transform, where the OFDM symbols are generated. Inverse fast Fourier transform (IFFT) converts frequency domain symbols to time-domain waveform and produces multiplexed orthogonal subcarriers.

The last stage is cyclic prefix addition, in which last M samples of the OFDM symbol are added to the beginning of the next one which reduces the effect of inter-symbol interference. The receiver implements the reverse order of the transmitter. In the first stage, the CP is removed from the OFDM symbol, followed by FFT stage. Then parallel-to-serial converter stage converts parallel data into serial sequence of OFDM symbols. The last stage symbol de-mapping converts the complex-valued number into the binary data.

4.3 UE and Simulation Environment

The UE shares the same components as the base stations (USRP and the host computer); the only difference is that the UE acts only as a receiver. UE position is changed in different scenarios. The simulation environment is run by the EB PROPCIM C8 radio channel emulator. EB Propsim C8 is a multichannel fading simulator that can simulate up to 16 independent or correlative propagation channels. It is used for testing wireless communication systems [28].

Figure 4.6 EB Propsim C8 [28]

The base stations and the UE are connected to the simulator via RF cables preceded by attenuators. The simulator controls the transmission variables and channel conditions — frequency of transmission, the bandwidth, sampling rate, the UE speed. The frequency, bandwidth, and sampling rate are kept the same as in USRP settings. Channel conditions are made idle for transmission; no channel loses introduced. UE speed is kept static and transmission power is –15 dBm.

Moreover, simulation scenarios and base station locations are drawn by the emulator, it also controls line of sight LOS and non-LOS transmission by introducing scatterers blocking LOS path.

The implementation aims to estimate the unknown location of UE in a narrowband IoT communication system. The UE is localized by nearby base stations using a trilateration algorithm. Where the distance is estimated based on TOA of NPRS signals. NPRS is generated and mapped on NB-IOT downlink waveform. The output grid is taken into OFDM transmitter to produce the OFDM symbols, CP is added, and IQ samples are produced. IQ samples are normalized, interleaved and printed to a file.

Base stations send the IQ samples carrying NPRS signal to the UE through the emulator. Synchronization between base stations is maintained by the OctoClock. The emulator adjusts the transmission parameters, channel conditions, and base station location. The NPRS is received and TOA is calculated. Distance from the UE is estimated for every base station. Known base station locations along with the estimated distance from the UE are given as input to the triangulation algorithm, which estimate the UE location.

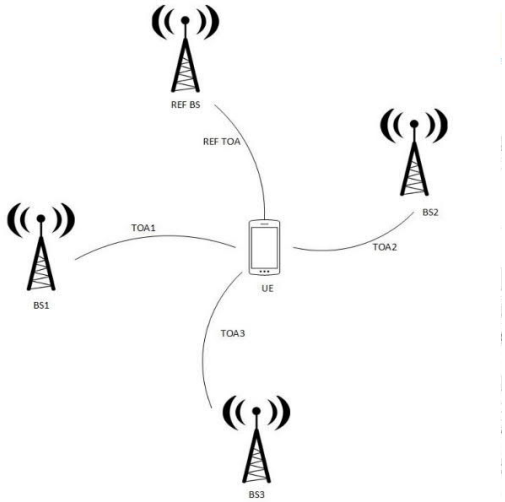


Figure 4.7 base stations sending signals to UE and calculating TOA

5 Simulation and Results

5.1 Simulation scenarios

As we discussed in Chapter 5, simulations are carried out by Propsim C8 emulator. Different scenarios are tested for different base station location settings and channel conditions. All scenarios use the location map in the figure below, known locations of base stations and UE depicted on the map as (x, y) coordinates. These coordinates are fed to the emulator. The emulator records the locations and calculates the received power of each base station accordingly.

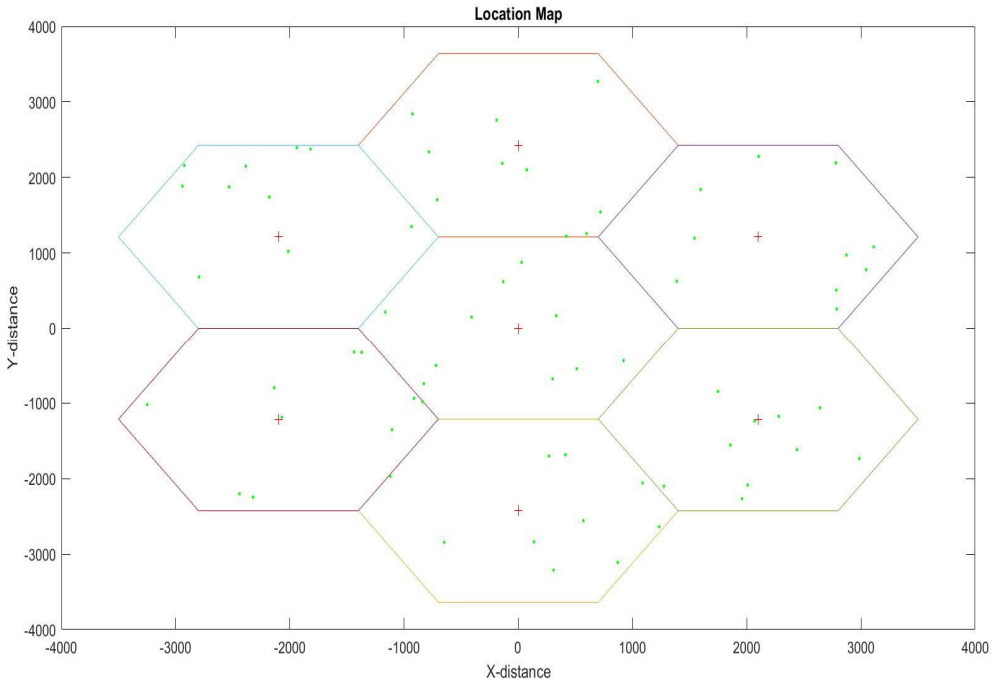


Figure 5.1 Location Map

The hexagonal shapes represent NB-IoT cells, and the red crosses in the middle of the cells represents Base stations while the green dots represent possible UE locations. In each scenario, we located different base stations and new UE location is selected and estimated. The base station sends the NPRS signal to the UE during the simulation. After that, the time delay is measured and used to estimate the distance to every base station. The UE location is estimated with triangulation and compared to the actual position we have selected from the map.

5.1.1 Scenario 1

This scenario aims to test the hypothesis that UE inside a triangular base station formation increase the accuracy of localization [29]. Three base stations used: A1, A2, A3, located at (-2100,1212), (2100,1212) and (0,2425) respectively. UE is at (718.1,1545) position and transmission power of base stations are A1 (-29.5dB), A2 (-23.7dB) , A3 (-35.5 dB). The transmission type is line of sight LOS with no scatterers.

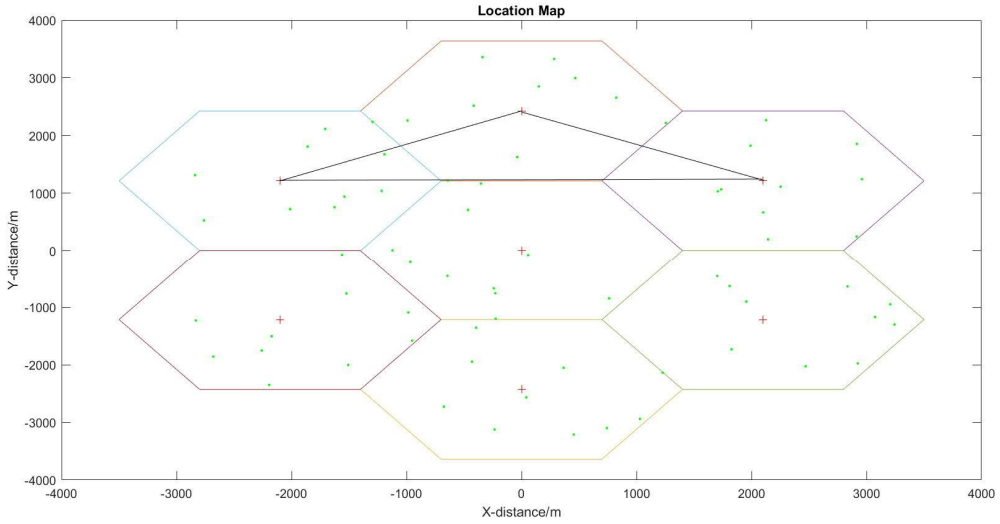


Figure 5.2 Scenario 1

The results obtained from measurements according to Figure 5.2. True distance, measured distance, and time delay are measured from each base station to the UE.

Table 5.1 Scenario 1 results

Results	Base stations		
	A1	A2	A3
True distance	1434.6 m	1170.3 m	2832.4 m
Delay	4.7 µsec	3.8 µsec	9.4 µsec
Estimated distance	1410 m	1140 m	2820 m
Error	24.57 m	30.25 m	12.37 m

Table 5.2 Scenario 1 estimated and actual UE location

True Location	Calculated location	Error
(718.1,1545)	(710,1531.7)	32.283 m

5.1.2 Scenario 2

This scenario aims to test the hypothesis that increasing the number of localizing base stations will increase localization accuracy. Four base stations are used; B1, B2, B3, B4, located at (-2100,1212), (2100,1212), (2100, -1212), and (-2100, -1212) respectively. UE is at (331.6,171.5) position and transmission power of base stations are A1 (-28.4dB), A2 (-18.8.7dB), A3 (-26.5 dB), A4 (-22.8 dB). The transmission type is LOS with no scatters.

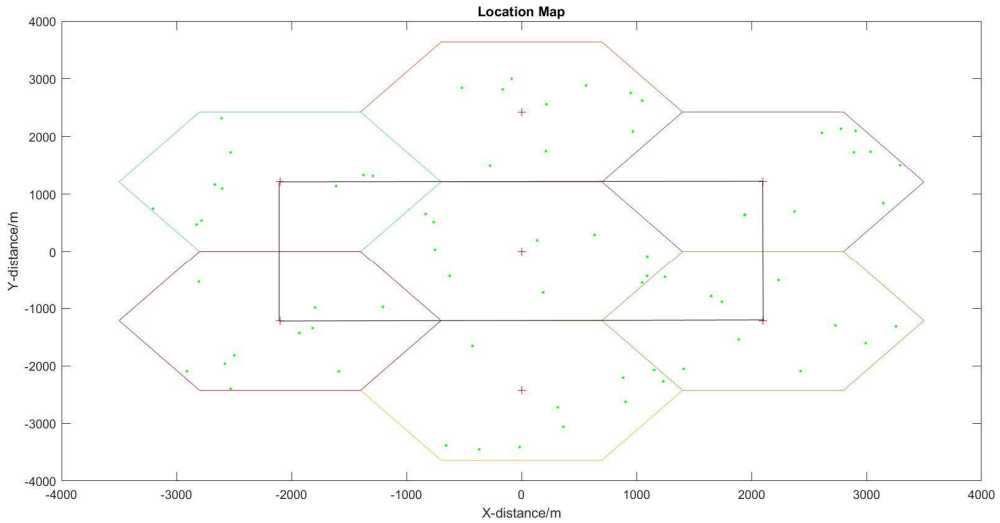


Figure 5.3 Scenario 2

The results obtained from measurements according to Figure 5.3. True distance, measured distance, and time delay are measured from each base station to the UE.

Table 5.3 Scenario 2 results

Results	Base stations			
	B1	B2	B3	B4
True distance	2649.2 m	2055.9 m	2239 m	2793.7 m
Delay	8.87 µsec	6.85 µsec	7.51 µsec	9.31 µsec
Estimated distance	2661 m	2055 m	2253 m	2793 m
Error	11.82 m	0.91 m	13.97 m	0.67 m

Table 5.4 Scenario 2 estimated and actual UE location

True Location	Calculated location	Error
(331.6,171.5)	(332.31,162.22)	9.30 m

5.1.3 Scenario 3

Line of sight is the main factor in determining the location in TOA algorithms. This scenario aims to block the line of sight by introducing scatters and investigate the effects on localization. Three base stations used; C1, C2, C3, located at (-2100,1212), (2100,1212) and (0,2425) respectively. UE is at (-1439, -321.6) position and transmission power of base stations are A1 (-20.2db), A2 (-23.2db), A3(-25.5) db. The transmission type is non-line-of-sight (NLOS) and scatterers.

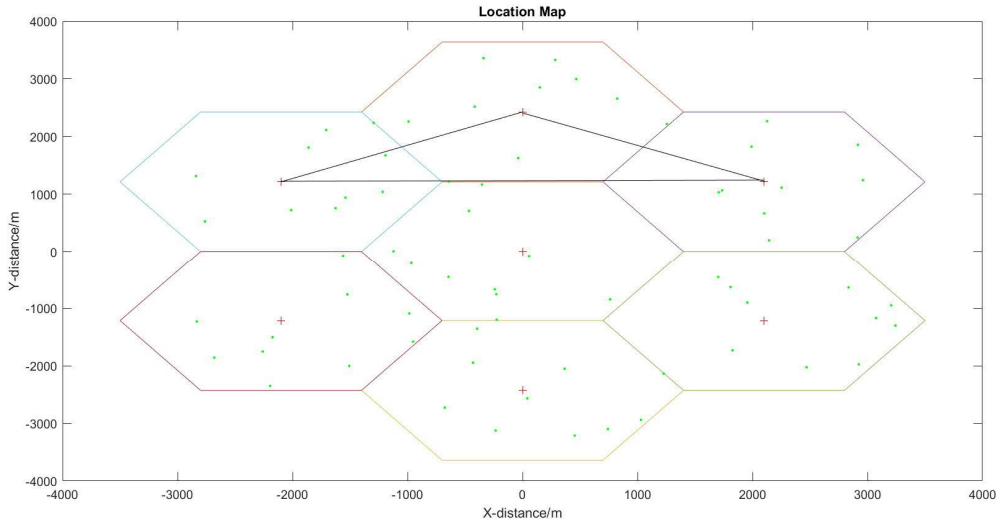


Figure 5.4 Scenario 3

The results obtained from measurements according to Figure 5.4. True distance, measured distance, and time delay are measured from each base station to the UE.

Table 5.5 Scenario 3 results

Results	Base stations		
	C1	C2	C3
True distance	1670 m	3857 m	3100.7 m
Delay	9 µsec	10.75 µsec	12.50 µsec
Estimated distance	2700 m	3225 m	3750 m
Error	1030 m	632 m	649.3 m

Table 5.6 Scenario 3 estimated and actual UE location

True Location	Calculated location	Error
(-1439, -321.6)	(-370.4, -2149.8)	2117.1 m

5.1.4 Scenario 4

In all previous scenarios, base stations were surrounding the UE while in this scenario all base station lies on a straight line. This scenario aims to test the effect of base station positions on localization of UE. Three base stations used; D1, D2, D3, located at (0,0), (2800,0) and (-2800,0) respectively. UE is at (28.76,876.6) position and transmission power of base stations are D1(-21.1dB), D2(-19.7dB), D3(-23.7dB). The transmission type is LOS with no scatterers.

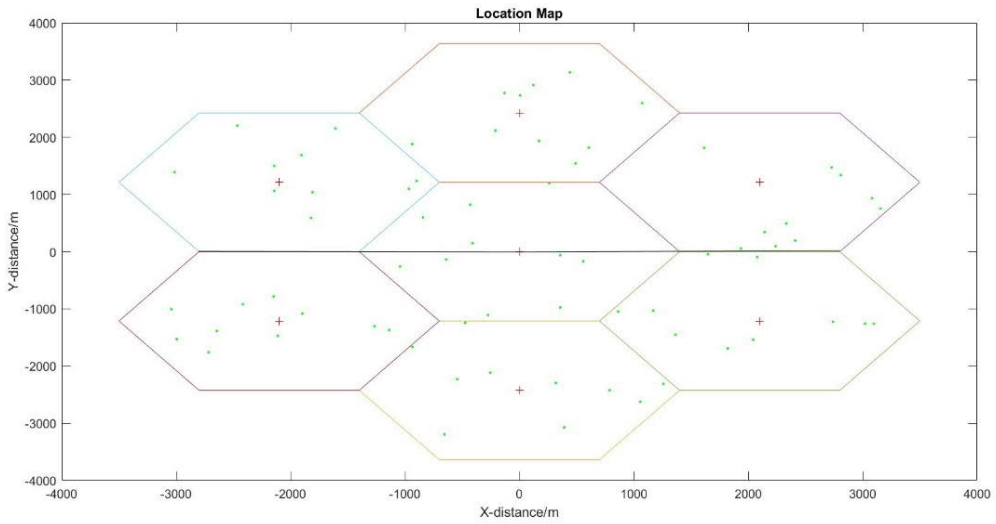


Figure 5.5 Scenario 4

The results obtained from measurements according to Figure 5.5. True distance, measured distance, and time delay are measured from each base station to the UE.

Table 5.7 Scenario 4 results

Results	Base stations		
	D1	D2	D3
True distance	877.3 m	2906.6 m	2961.5 m
Delay	9.9 µsec	6.85 µsec	9.3 µsec
Estimated distance	2970 m	2055 m	2790 m
Error	2096.7 m	851.6 m	171.50 m

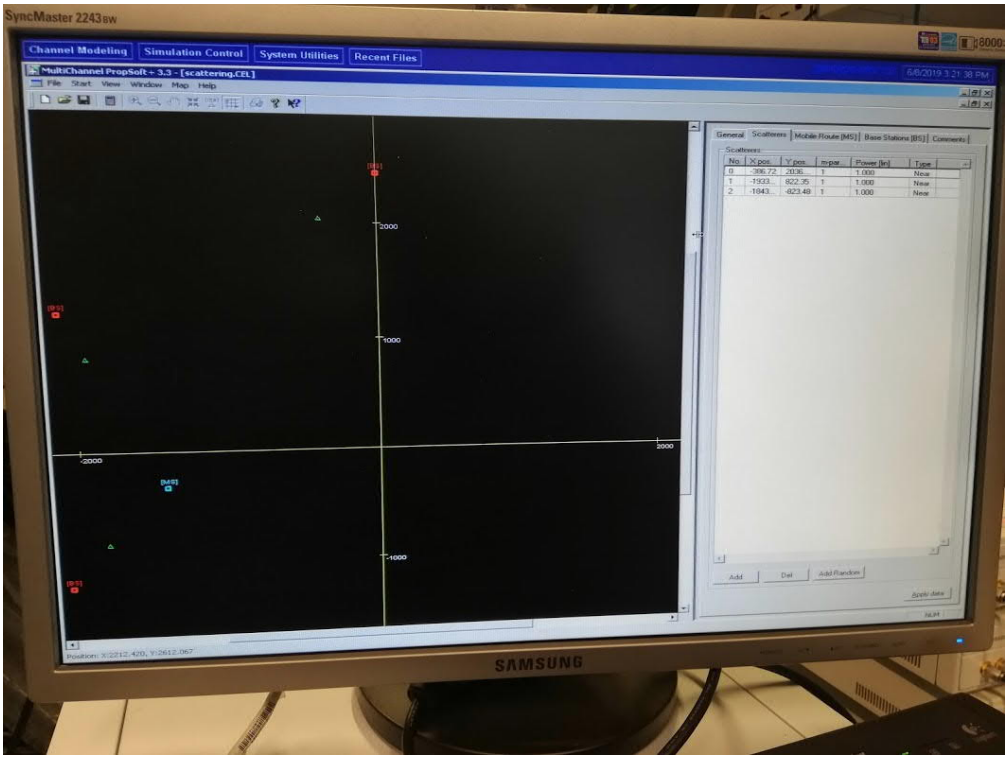


Figure 5.6 Scenario 3 NLOS (base stations are red, UE is blue, and scatterers are green)

Figure 5.7 Scenario 2 on emulator (base stations are red, UE is blue)

5.2 Results and Discussion

Localization using the TOA algorithm is most sensitive to time measurement errors, and each Base station error contribute to more inaccurate results. Inaccurate TOA at a Base station will result in an error in the estimated distance between UE and that Base, consequently accumulated error in the final estimated location. Another less obvious factor is the geometry of measurement. The relative base station to UE geometry plays a vital role in the UE localization accuracy; this is called geometrical dilution of precision (GDOP) [30].

Scenarios 1 and 2 test the hypothesis represented in [29], they mention that UE localization accuracy increases and GDOP decrease when the UE is in the center of the localizing base stations. Scenarios 1 and 2 have the highest localization accuracies in all the scenarios with errors of (32.28 m) and (9.3 m) respectively.

Scenario 2 test another hypothesis represented in [29], which states that increasing the number of base stations increases localization accuracy. Scenario 2 has one more base station than scenario 1, which totals four. Scenario 2 has the lowest localization distance error (9.3 m), which accords with the theory. Scenario 1 and 2 share some significant attributes. First, they both have LOS between UE and Base stations. Secondly, the UE is in the center surrounded by Base stations in both cases. Leading to both scenarios having higher accuracy in localization among all other scenarios. Scenario 2 provides better efficiency than Scenario 1 since it has more base stations for localization.

Scenario 3 test the hypothesis in [16], which mentions that NLOS decrease localization accuracy. The signal travelling along the NLOS path may have covered far more considerable distances than LOS signal, thus affecting time of flight and producing biased TOA. The localization error in this scenario confirms it, (2117.1 m) distance error which is far worse than the first two scenarios, and especially compared with scenario 1(32.28 m) has the same number of base stations.

Scenario 4 is the opposite of scenario 1 in which base stations are not surrounding the UE. we could not calculate the final location of the UE using the algorithm discussed in [18] because base stations falling all in the same line produce a multi-alteration problem that has infinitely many solutions [18]. Although we did not estimate the final location here, we can see from Table 6.7 that the accuracy of the estimated distance between each base station and the UE is low. In comparison with scenario 1, the location error of scenario 4 base station to UE estimated distance is more than 10 folds.

A significant factor that could improve localization accuracy in all the scenarios is increasing the time measurement sensitivity from microseconds to nanoseconds. As the estimated distance is time-dependent and the signal travels with the speed of light velocity. Increasing time-sensitivity will yield in better positioning accuracy. Added to that, increasing the complexity of TOA estimation techniques would enhance positioning accuracy [16]. TOA estimation used is in this thesis, other more complex TOA estimation techniques could be used (such as, deconvolution based), if a tradeoff between complexity and accuracy could be managed.

Table 5.8 Emulation results

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
No of base stations	3	4	3	3
LOS / NLOS	LOS	LOS	NLOS	LOS
scatterers	no	no	yes	no
Error	32.28m	10m	211.71m	undefined

6 Conclusion and future work

We tested three central localization hypotheses in this NB-IoT SDR implementation; First, LOS and NLOS effect on localization, Secondly, the impact of increasing the number of base stations involved in localization, Thirdly, the relative position between the UE and the base stations involved in the localization. The addition of scatters has tested both LOS and NLOS scenarios. LOS cases have shown to produce more accurate results than NLOS as the LOS signal takes the shortest path between the UE and the base station, giving more accurate TOA estimation and therefore more accurate location estimation. Increasing the number of base stations has also shown to improve the overall UE localization accuracy. Nevertheless, it will increase the cost of computation and the total power used in localization. Finally, the relative position between the UE and the base station has shown better results when the localizing base stations surround the UE.

Scenarios 1 and 2 have achieved the positioning accuracy requirement of 50 m horizontal accuracy for localization in NB-IoT [14]. Applications for such accuracy would better suite tracking or mostly static monitoring objects or with no frequent change in position such as, warehouse tracking, safety monitoring in industry, or forest fire fighting. Although the required NB-IoT positioning accuracy has been reached in the simulations, it is still far from reality. Fundamental elements have been kept idle in these simulations that would have dramatically influenced the results, such as, Signal attenuation from weather or obstacles, interference from other signals, multipath effects. Moreover, the system was accurately synchronized in this implementation, but synchronization inaccuracies are inevitable. In the future, we can test all these elements to ensure close to real results.

A further extension of this work can be for indoor positioning, as this is a closely related topic but not included. Many challenges could face indoor positioning, especially in NB-IoT. NB-IoT is bandwidth sensitive with 200 kHz channel, which is not helpful in intensive multipath environments. Finally, localization in this thesis has been two-dimensional. In the future three-dimensional localization could be tested, which would increase the localization spectrum of IoT device such as, drones.

7 References

[1] International Telecommunication Union Internet Reports, "The Internet of Things," 2005.

[2] F. J. Dian, R. Vahidnia and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey," *IEEE Access,* vol. 8, p. 69200–69211, 2020.

[3] 3GPP TS36.211, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and modulation".*3GPP TS 36.211 version 14.2.0 Release 14.*

[4] D. Miorandi, S. Sicari, F. D. Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks,* 2012.

[5] Edureka, "IoT Applications," [Online]. Available: https://www.edureka.co/blog/iot-applications/. [Accessed July 2020].

[6] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya and M. Conti, "IoT-enabled smart lighting systems for smart cities," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 2018.

[7] Vaisala oyj, "ViewLinc Monitoring , Alarming and Reporting Software," Vaisala, [Online]. Available: https://www.vaisala.com/en/products/instruments-sensors-and-other-measurement-devices/vainet.

[8] LoRa Alliance, "Home Page lora-alliance," The LoRa Alliance® , 2015. [Online]. [Accessed July 2020].

[9] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman and H. S. Razaghi, "A primer on 3GPP narrowband Internet of Things," *IEEE communications magazine,* vol. 55, p. 117–123, 2017.

[10] Ericsson, "NB-IoT: a sustainable technology for connecting billions of devices," [Online]. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/nb-iot-a-sustainable-technology-for-connecting-billions-of-devices. [Accessed July 2020].

[11] 3GPP TS36.211, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and modulation," *3GPP TS 36.211 version 13.2.0 Release 13.*

[12] A. Hoglund, X. Lin, O. Liberg, A. Behravan, E. A. Yavuz, M. Van Der Zee, Y. Sui, T. Tirronen, A. Ratilainen and D. Eriksson, "Overview of 3GPP release 14 enhanced NB-IoT," *IEEE network,* vol. 31, p. 16–22, 2017.

[13] S. Ullerstig, "Know the difference between NB-IoT vs. Cat-M1 for your massive IoT deployment," Ericsson, 07 February 2019. [Online]. Available: https://www.ericsson.com/en/blog/2019/2/difference-between-nb-iot-cat-m1.

[14] X. Lin, J. Bergman, F. Gunnarsson, O. Liberg, S. M. Razavi, H. S. Razaghi, H. Rydn and Y. Sui, "Positioning for the Internet of Things: A 3GPP Prespective," *IEEE Communications Magazine,* 2017.

[15] A. M. H. Khalel, *Position location techniques in wireless communication systems,* 2010.

[16] S. A.Zekavat and R. Buehrer, HANDBOOK OF POSITION LOCATION : Theory, Practice, and Advances, WILEY, 2012.

[17] E. Tou, "Triangulation in the Plane," GeoGebra, [Online]. Available: https://www.geogebra.org/m/hx6VeeWk.

[18] A. Norrdine, "An ALgebric Solution to the Multilateration Problem," in *International Conference on Indoor Positioning and Indoor Navigation*, 2012.

[19] A. K. Paul and T. Sato, "Localization in wireless sensor networks: A survey on algorithms, measurement techniques, applications and challenges," *Journal of Sensor and Actuator Networks,* vol. 6, p. 24, 2017.

[20] Y. Wang, X. Yang, Y. Zhao, Y. Liu and L. Cuthbert, "Bluetooth positioning using RSSI and triangulation methods," in *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, 2013.

[21] Ettus Research, "Ettus Research the leader in Software Defined Radio," National Instruments, October 2019. [Online]. [Accessed October 2019].

[22] Ettus Reseach, "UHD Ettus-Knowledge Base," National Instruments, [Online]. Available: https://kb.ettus.com/UHD. [Accessed 1 October 2019].

[23] Ettus Research, "USRP N200," National Instruments, 2019. [Online]. Available: https://www.ettus.com/all-products/un200-kit/. [Accessed 21 August 2019].

[24] Etttus Research, "OctoClock Clock Distribution Module with GPSDO," National Instruments, 2019. [Online]. [Accessed August 2019].

[25] MATLAB, "LTE Toolbox-MATLAB," 2019. [Online]. Available: https://se.mathworks.com/products/lte.html. [Accessed August 2019].

[26] MATLAB LTE ToolBox, "NB-IoT Downlink Waveform Generation," 2019. [Online]. Available: https://se.mathworks.com/help/lte/examples/nb-iot-downlink-waveform-generation.html. [Accessed August 2019].

[27] H. Zarrinkoub, Understanding LTE with MATLAB, Massachusetts: WILEY, 2014.

[28] Elektrobit Corporation, "EB Propsim C8 Radio Channel EMulator," 2009. [Online]. Available: http://read.pudn.com/downloads765/doc/3037695/EB%20Propsim%20C8_2.3.pdf. [Accessed june 2019].

[29] S. Fischer, "Observed Time Difference Of Arrival Positioning in 3GPP LTE," Qualcom Technologies, INC, 2014.

[30] R. Langely, "Dilution of Percision," *GPS World,* vol. 10, pp. 52-59, 1999.

[32] E.-j. Zhong and T.-z. Huang, "Geometric dilution of precision in navigation computation," in *International Conference on Machine Learning and Cybernetics*, 2006.

[33] I. Olofsson, *Enhancements in LTE OTDOA positioning for multipath environments,* 2016.

[34] S. Bremberg, *Calibration of Multilateration Positioning Systems via Nonlinear Optimization,* 2015.

[35] A. Berg and A. R. M. Michal Stala, "OTDOA-based positioning in NB-IoT," *Ph. D. dissertation,* 2017.

[36] O. Khalil, "A USE CASE OF LOW POWER WIDE AREA NETWORKS IN FUTURE 5G HEALTHCARE APPLICATIONS," 2018.

[37] K.-C. Chen and S.-Y. Lien, "Machine-to-machine communications: Technologies and challenges," *Ad Hoc Networks,* vol. 18, p. 3–23, 2014.